UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/735,581	12/12/2003	Sudarshan Palliyil	JP920030275US1	2542

39903 7590 12/07/2007
IBM ENDICOTT (ANTHONY ENGLAND)
LAW OFFICE OF ANTHONY ENGLAND
PO Box 5307
AUSTIN, TX 78763-5307

EXAMINER	
ZEE, EDWARD	
ART UNIT	PAPER NUMBER
2135	
MAIL DATE	DELIVERY MODE
12/07/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/735,581	PALLIYIL ET AL.	
	Examiner	Art Unit	
	Edward Zee	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on *07 August 2007*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *3-10 and 30-48* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *3-10 and 30-48* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *15 July 2007* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This is in response to the amendment filed on August 7th, 2007. Claims 1, 2 and 11-29 have been cancelled; Claims 3-10 have been amended; Claims 30-48 have been added; and Claims 3-10 and 30-48 are pending and have been considered below.

Drawings

2. The drawings were received on 7/15/07. These drawings are acceptable for examination.

Specification

3. The amendments to the specification filed on 7/15/07 have been considered and effectively overcome the previous objections to the specification. Therefore, the previous objections have been withdrawn.

Claim Objections

4. Claim 30 is objected to because of the following informalities: the Examiner notes that lines 6-7 of the instant claim reads, *"storing the computed set of first hash values, wherein the storing includes: computing at least second hash values for the replicas of the resource, wherein the... "*, but should in fact read, *"storing the computed set of hash values; wherein the method further comprises: computing at least second hash values for the replicas of the resource..."* and will be considered in this manner. Appropriate correction is required.

Claim Rejections - 35 USC § 112

5. The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

6. Claim 30 is rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention.

The Examiner notes that lines 6-7 of the instant claim reads:

"storing the computed set of first hash values, ***wherein the storing includes:*** *computing at least second hash values for the replicas of the resource, wherein the..."*

which does not appear to be supported by the original specification and thus contains new matter.

7. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

8. Claims 30, 31, 40, 5, 34, 43, 6, 35, 44, 7, 36, 45, 9, 38 and 47 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

9. Claim 30 recites the limitations "the time stamps", "the hash values" and "the hash value comparison" in lines 10 and 13. There is insufficient antecedent basis for this limitation in the claim.

10. Claim 31 recites the limitation "the time stamps", "the hash values", "the hash value comparison" and "the predetermined number of changes" in lines 12, 15 and 21. There is insufficient antecedent basis for this limitation in the claim.

11. Claim 40 recites the limitation "the time stamps...computed at successive times", "the hash values" and "the hash value comparison" in lines 12 and 15. There is insufficient antecedent basis for this limitation in the claim.

12. Claim 5, 34 and 43 recites the limitation "the predetermined number" in line 3. There is insufficient antecedent basis for this limitation in the claim.

13. Claim 6, 35 and 44 recites the limitation "the predetermined number" in line 4. There is insufficient antecedent basis for this limitation in the claim.

14. Claim 7, 36 and 45 recites the limitation "the predetermined number" in lines 3-4. There is insufficient antecedent basis for this limitation in the claim.

15. Claim 9, 38 and 47 recites the limitation "the predetermined number" in line 4. There is insufficient antecedent basis for this limitation in the claim.

16. Due to the numerous 35 U.S.C. 112, second paragraph issues throughout all the claims, the claims have not been checked to the extent necessary to determine the presence of all possible issues. Applicant's cooperation is requested in correcting any errors of which applicant may become aware in the claims.

Claim Rejections - 35 USC § 103

17. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

18. Claims 3-5, 9, 30-34, 38, 40-43 and 47 are rejected under 35 U.S.C. 103(a) as being unpatentable over Glover (6,763,466) in view of Bates et al. (DE 10126752 A1).

Claim 30: Glover discloses a method within a network having a vulnerability, the method comprising the steps of:

a. computing first hash values derived from and representing a plurality of replicas of a resource, wherein the replicas of the resource are stored on respective data processing systems within a network*(ie. AV state information includes parameters such as checksum and last-modified date stamp)* [column 6, lines 24-26];

b. storing the computed set of first hash values*(ie. anti-virus program stores AV state information in reserved fields)* [column 6, lines 17-24];

c. computing at least second hash values for the replicas of the resource, wherein the computing of the at least second hash values is at a time after the computing of the first hash values*(ie. obtains the AV state information from the reserved fields and compares the saved AV state information with the corresponding information currently associated with the file)* [column 6, lines 43-47];

d. determining if the file needs to be re-scanned based on the comparison of the AV state information(ie. hash values, date stamp, etc.) [column 8, lines 17-19].

However, Glover does not explicitly disclose:

a. computing, responsive to comparing a set of time stamps and a set of hash values computed at successive times, a time duration during which a set of hash values of each respective the replicas of the resource remained unchanged;

b. and detecting for a current time, responsive to the hash value comparison indicating that at least one of the replicas of the resource have changed from one time to the current time, whether the changed replicas of the resource at the current time indicate a vulnerability, wherein the detecting comprises detecting whether the computed time duration prior to the current time exceeds a predetermined time duration;

c. wherein the method further comprises presenting a message for a user indicating a vulnerability, wherein the presenting is responsive to the predetermined time duration being exceeded.

Nonetheless, Bates et al. discloses a similar method and further discloses:

a. computing, responsive to comparing a set of time stamps and previous virus scan data, a time duration during which a set of virus scan data of each respective the replicas of the resource remained unchanged*(ie. virus criterion, not checked in last 14 days)* [figure 7];

b. and detecting for a current time, responsive to the virus scan data comparison indicating that at least one of the replicas of the resource have changed from one time to the current time, whether the changed replicas of the resource at the current time indicate a vulnerability, wherein the detecting comprises detecting whether the computed time duration prior to the current time exceeds a predetermined time duration*(ie. virus found in last 7 days or not checked in last 14 days, etc.)* [figure 7];

c. wherein the method further comprises presenting a message for a user indicating a vulnerability, wherein the presenting is responsive to the predetermined time duration being exceeded*(ie. report options, notify)* [figure 7].

Therefore, it would have been obvious to one of ordinary skill in the art at the time of invention to further modify the detection scheme disclosed by Glover with the features disclosed by Bates et al.. One would have been motivated to do so in order to flag files which have either not been scanned for an extended period of time, or files which have been infected within a certain period of time as being potentially untrustworthy.

Claim 31: Glover discloses an apparatus comprising a processor and a storage device connected to the processor, wherein the storage device has stored thereon a program, wherein the processor is operative to execute instructions of the program to implement a method comprising the steps of:

a. computing first hash values derived from and representing a plurality of replicas of a resource, wherein the replicas of the resource are stored on respective data processing systems within a network*(ie. AV state information includes parameters such as checksum and last-modified date stamp)* [column 6, lines 24-26];

b. storing the computed set of first hash values*(ie. anti-virus program stores AV state information in reserved fields)* [column 6, lines 17-24];

c. computing at least second hash values for the replicas of the resource, wherein the computing of the at least second hash values is at a time after the computing of the first hash values*(ie. obtains the AV state information from the reserved fields and compares the saved AV state information with the corresponding information currently associated with the file)* [column 6, lines 43-47];

d. determining if the file needs to be re-scanned based on the comparison of the AV state information(ie. hash values, date stamp, etc.) [column 8, lines 17-19].

However, Glover does not explicitly disclose:

a. computing, responsive to comparing the time stamps and the hash values computed at successive times, a time duration during which the hash values of each respective the replicas of the resource remained unchanged;

b. detecting for a current time, responsive to the hash value comparison indicating that at least one of the replicas of the resource has changed from one time to the current time, whether the at least one changed replicas of the resource at the current time indicates a vulnerability, wherein the detecting comprises detecting whether the computed time duration prior to the current time exceeds a predetermined time duration;

c. wherein the method further comprises presenting a message for a user indicating a vulnerability, wherein the presenting is responsive to the predetermined number of changed replicas of the resource being exceeded.

Nonetheless, Bates et al. discloses a similar apparatus and further discloses:

a. computing, responsive to comparing a set of time stamps and previous virus scan data, a time duration during which a set of virus scan data of each respective the replicas of the resource remained unchanged*(ie. virus criterion, not checked in last 14 days)* [figure 7];

b. and detecting for a current time, responsive to the virus scan data comparison indicating that at least one of the replicas of the resource have changed from one time to the current time, whether the changed replicas of the resource at the current time indicate a vulnerability, wherein the detecting comprises detecting whether the computed time duration prior to the current time exceeds a predetermined time duration*(ie. virus found in last 7 days or not checked in last 14 days, etc.)* [figure 7];

c. wherein the method further comprises presenting a message for a user indicating a vulnerability, wherein the presenting is responsive to a predetermined number of changed being exceeded*(ie. report options, notify, if virus was ever found, wherein the predetermined number in this case may equal zero, thus if a virus has been found in the past zero would be exceeded)* [figure 7].

Therefore, it would have been obvious to one of ordinary skill in the art at the time of invention to further modify the detection scheme disclosed by Glover with the features disclosed by Bates et al.. One would have been motivated to do so in order to flag files which have either not been scanned for an extended period of time, or files which have been infected within a certain period of time as being potentially untrustworthy.

Claim 40: Glover discloses a computer program product, stored on a tangible, computer readable medium, said computer program product having instructions for execution by a computer system, wherein the instructions, when executed by the computer system, cause the computer system to implement a method comprising the steps of:

a. computing first hash values derived from and representing a plurality of replicas of a resource, wherein the replicas of the resource are stored on respective data processing systems within a network*(ie. AV state information includes parameters such as checksum and last-modified date stamp)* [column 6, lines 24-26];

b. storing the computed set of first hash values and time stamps for the first hash values*(ie. anti-virus program stores AV state information in reserved fields)* [column 6, lines 17-24];

c. computing at least second hash values for the replicas of the resource, wherein the computing of the at least second hash values is at a time after the computing of the first hash values*(ie. obtains the AV state information from the reserved fields and compares the saved AV state information with the corresponding information currently associated with the file)* [column 6, lines 43-47];

d. determining if the file needs to be re-scanned based on the comparison of the AV state information(ie. hash values, date stamp, etc.) [column 8, lines 17-19].

However, Glover does not explicitly disclose:

a. computing, responsive to comparing the time stamps and the hash values computed at successive times, a time duration during which the hash values of the replicas of the resource remained unchanged;

b. and detecting for a current time, responsive to the hash value comparison indicating that at least one of the replicas of the resource has changed from one time to the current time, whether the at least one changed replica of the resource at the current time indicates a vulnerability, wherein the detecting comprises detecting whether the computed time duration prior to the current time exceeds a predetermined time duration;

c. wherein the method further comprises presenting a message for a user a vulnerability, wherein the presenting is responsive to the predetermined time duration being exceeded.

Nonetheless, Bates et al. discloses a computer program product and further discloses:

a. computing, responsive to comparing a set of time stamps and previous virus scan data, a time duration during which a set of virus scan data of each respective the replicas of the resource remained unchanged*(ie. virus criterion, not checked in last 14 days)* [figure 7];

b. and detecting for a current time, responsive to the virus scan data comparison indicating that at least one of the replicas of the resource have changed from one time to the current time, whether the changed replicas of the resource at the current time indicate a vulnerability, wherein the detecting comprises detecting whether the computed time duration prior to the current time exceeds a predetermined time duration*(ie. virus found in last 7 days or not checked in last 14 days, etc.)* [figure 7];

c. wherein the method further comprises presenting a message for a user indicating a vulnerability, wherein the presenting is responsive to the predetermined time duration being exceeded*(ie. report options, notify)* [figure 7].

Therefore, it would have been obvious to one of ordinary skill in the art at the time of invention to further modify the detection scheme disclosed by Glover with the features disclosed by Bates et al.. One would have been motivated to do so in order to flag files which have either not been scanned for an extended period of time, or files which have been infected within a certain period of time as being potentially untrustworthy.

Claims 3, 32 and 41: Glover and Bates et al. disclose a method, apparatus and computer program product of claims 30, 31 and 40, and Glover further discloses that the vulnerability includes a vulnerability to a computer virus [column 1, line 35].

Claims 4, 33 and 42: Glover and Bates et al. disclose a method, apparatus and computer program product of claims 30, 31 and 40, and Glover further discloses that the vulnerability includes a vulnerability to computer hacking [column 1, line 35].

Claims 5, 34 and 43: Glover and Bates et al. disclose a method, apparatus and computer program product of claims 30, 31 and 40, but Glover does not explicitly disclose classifying the

data processing systems storing replicas of the resource as vulnerable, wherein the classifying is responsive to the predetermined number of changed replicas of the resource being exceeded and the predetermined time duration being exceeded.

However, Bates et al. further discloses classifying the data processing systems storing replicas of the resource as vulnerable, wherein the classifying is responsive to the predetermined number of changed replicas of the resource being exceeded and the predetermined time duration being exceeded*(ie. if virus has ever been found for a particular result, classify the result by either excluding it, notifying, or disabling it)* [figure 7].

Therefore, it would have been obvious to one of ordinary skill in the art at the time of invention to further modify the detection scheme disclosed by Glover with the features disclosed by Bates et al.. One would have been motivated to do so in order to flag files which have either not been scanned for an extended period of time, or files which have been infected within a certain period of time as being potentially untrustworthy.

Claims 9, 38 and 47: Glover and Bates et al. disclose a method, apparatus and computer program product of claims 30, 31 and 40, but Glover does not explicitly disclose the steps comprising sending a notification of the vulnerability to each data processing system storing a replica of the resource, wherein the sending is responsive to the predetermined number of changed replicas of the resource being exceeded and the predetermined time duration being exceeded.

However, Bates et al. further discloses disclose the steps comprising sending a notification of the vulnerability to each data processing system storing a replica of the resource, wherein the sending is responsive to the predetermined number of changed replicas of the

resource being exceeded and the predetermined time duration being exceeded*(ie. if virus has ever been found for a particular result or exceeds a particular time limit, notify user)* [figure 7].

Therefore, it would have been obvious to one of ordinary skill in the art at the time of invention to further modify the detection scheme disclosed by Glover with the features disclosed by Bates et al.. One would have been motivated to do so in order to flag files which have either not been scanned for an extended period of time, or files which have been infected within a certain period of time as being potentially untrustworthy.

19. **Claims 6-8, 10, 35-37, 39, 44-46 and 48 are rejected under 35 U.S.C. 103(a) as being unpatentable over Glover (6,763,466) in view of Bates et al. (DE 101 26 752 A 1) and further in view of Radatti (7,143,113).**

Claims 6, 35 and 44: Glover and Bates et al. disclose a method, apparatus and computer program product of claims 30, 31 and 40, but neither explicitly disclose replacing the replica of the resource at each of the data processing systems storing a replica of the resource, wherein the replacing is responsive to the predetermined number of changed replicas of the resource being exceeded and the predetermined time duration being exceeded.

However, Radatti discloses a similar method, apparatus and computer program product and further discloses that a system that has been altered may be restored by replacing the affected file(s) with a known good copy of the file(s) [column 7, lines 59-65].

Therefore, it would have been obvious to one of ordinary skill in the art at the time of invention to replace the replicas disclosed by Glover and Bates et al. if it has been deemed to be compromised. One would have been motivated to do so in order to increase the security of the system by removing or repairing all points of vulnerability within the system.

Claims 7, 36 and 45: Glover and Bates et al. disclose a method, apparatus and computer program product of claims 30, 31 and 40, but neither explicitly disclose patching the replica of the resource at each of the data processing systems storing a replica of the resource, wherein the patching is responsive to the predetermined number of changed replicas of the resource being exceeded and the predetermined time duration being exceeded.

However, Radatti discloses a similar method, apparatus and computer program product and further discloses further discloses a system modification tool to restore the system to a secure system state [column 8, lines 61-67].

Therefore, it would have been obvious to one of ordinary skill in the art at the time of invention to patch the replicas disclosed by Glover and Bates et al. if it has been deemed to be compromised. One would have been motivated to do so in order to increase the security of the system by removing or repairing all points of vulnerability within the system.

Claims 8, 37 and 46: Glover and Bates et al. disclose a method, apparatus and computer program product of claims 7, 36 and 45, but neither explicitly disclose:

a. prior to patching the replica of the resource, comparing a set of hash values representing all pre-requisite programs of patch code with a stored set of hash values;

b. and in response to identification of matching hash codes for all pre-requisite programs, determining that said patching of the replica of the resource should proceed.

However, Radatti further discloses:

a. patching the replica of the first resource with patch code. The examiner notes it is inherent that a patch code is used when patching a file;

b. comparing the hashed transmitted content to determine whether the content has maintained pretransmission integrity [column 10, lines 20-24], but does not explicitly disclose comparing a set of hash values representing all pre-requisite programs of the patch code with the stored set of hash values to identify matching hash codes; nor that in response to identification of matching hash codes for all pre-requisite programs, determining that said patching of the replica of the first resource with the patch code should proceed.

Therefore, it would have been obvious to one of ordinary skill in the art at the time of invention to verify the integrity of a patch code before proceeding with the patching. One would have been motivated to do so in order to verify that the patch code being used to repair a file has not been compromised during transmission in order to maintain integrity within the system.

Claims 10, 39 and 48: Glover and Bates et al. disclose a method, apparatus and computer program product of claims 9, 38 and 47, but neither explicitly disclose selecting a sequence of vulnerability-resolution instructions relevant to the vulnerability and including the selected instructions within the notification sent to each data processing system.

However, , Radatti discloses a similar method, apparatus and computer program product and further discloses further discloses responding to the determination of respective systems storing replicas of the first resource by selecting a sequence of vulnerability-resolution instructions relevant to the vulnerability*(manually or automatically sending infected file to an antivirus or similar product)* [column 7, lines 30-35], but does not explicitly disclose including the selected instructions within the notification sent to each data processing system and including the step of receiving, from a remote data processing system, at least one hash value representing a first resource associated with a vulnerability together with vulnerability resolution information.

Therefore, it would have been obvious to one of ordinary skill in the art at the time of invention to send a hash value representing a first resource associated with a vulnerability and resolution instructions to facilitate the repair. One would have been motivated to do so in order to enable a user to manually restore any compromised files by themselves.

Response to Arguments

20. Applicant's arguments with respect to claims 30, 31 and 40 have been considered but are moot in view of the new ground(s) of rejection.

Conclusion

21. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. Bates et al. (6,721,721) is the issued U.S. patent of which DE 101 26 752 A1 claims priority from.

22. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event,

however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Edward Zee whose telephone number is (571) 270-1686. The examiner can normally be reached on Monday through Thursday 9:00AM-5:00PM EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Y. Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

EZ
November 28th, 2007

KIM VU
PATENT EXAMINER
TECHNOLOGY CENTER 2100